pfSense - Bug #4379

Remove CGN (RFC6598) address space from "private networks"

02/05/2015 12:34 PM - Kill Bill

Status:	Resolved	**Start date:**	02/05/2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:	2.2.1		
Plus Target Version:		**Affected Version:**	All
Release Notes:	Default	**Affected Architecture:**	All

Description

No need to filter this in both places, this is really the same thing like RFC1918 ranges.

Forum thread: https://forum.pfsense.org/index.php?topic=88215.0

Associated revisions

Revision 2dfe7846 - 02/05/2015 01:47 PM - Chris Buechler

remove CGN from "Block private networks" as it was in 2.0x and earlier releases since it specifically notes RFC 1918 and CGN is more bogon. Ticket #4379

Revision e4610d66 - 02/05/2015 03:09 PM - Chris Buechler

remove CGN from "Block private networks" as it was in 2.0x and earlier releases since it specifically notes RFC 1918 and CGN is more bogon. Ticket #4379

History

#1 - 02/05/2015 03:08 PM - Chris Buechler

- Subject changed from Remove CGN (RFC6598) address space from bogons to Remove CGN (RFC6598) address space from "private networks"

- Status changed from New to Resolved

- Target version set to 2.2.1

since block private specifically says RFC 1918, it's more valid as bogon than private, I removed it from private.

#2 - 02/05/2015 05:01 PM - Kill Bill

I'm not using either of these, so I pretty much don't care either way, but... fixing the description and nuking this from bogons leaves people with usable bogon rules that are blocking **loads** of other stuff. When you leave CGN in bogons, people on CGN just cannot use those at all since you cannot override it in any reasonable way (still no way to move those rules). Hmmm.

#3 - 02/05/2015 05:09 PM - Chris Buechler

Bogons and block private only applies to traffic sourced on the WAN in question. Where you're on CGN, you pretty much never want to allow traffic sourced from CGN subnets in. There is never any need to disable that for outbound traffic regardless of whether your WAN is CGN or private or bogon.

there is a feature request open to allow moving the rules, which could be handy in some limited circumstances (mostly to block matching traffic with no logging without completely disabling the rule).

#4 - 02/05/2015 05:16 PM - Kill Bill

Yes, of course. I think we don't understand each other. I can trivially create a RFC1918 alias and place that rule whereever I want (it's 3 CIDRs, or 4 including the CGN address space). Not exactly the case with bogons{,v6}. So, this CGN address space is effectively burried among loads of completely unrelated IP ranges. As long as you leave it there, you render the entire bogons list unusable for anyone behind CGN. Not talking about outbound traffic at all.

#5 - 02/11/2015 07:20 PM - Chris Buechler

it's only unusable where you need to allow traffic into WAN that's sourced from CGN space. Which in nearly all cases is nothing. I think you're misunderstanding what block bogons does, it most certainly doesn't "render the entire bogons list unusable for anyone behind CGN."